UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/696,621	10/30/2003	Makoto Fujiwara	60188-694	5601

7590 07/28/2008

Jack Q. Lever, Jr.
McDERMOTT, WILL & EMERY
600 Thirteenth Street, N.W.
Washington, DC 20005-3096

EXAMINER	
COLIN, CARL G	

ART UNIT	PAPER NUMBER
2136	

MAIL DATE	DELIVERY MODE
07/28/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/696,621	FUJIWARA ET AL.	
	Examiner	Art Unit	
	CARL COLIN	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *23 April 2008*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-8* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-8* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *see attached*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Response to Arguments

1. In communications filed on 4/23/2008, applicant has amended claims 1, 2, 4, and 8 and cancels claims 9-11. The following claims 1-8 are presented for examination

1.1 In response to communications filed on 4/23/2008, the double patenting rejection has been withdrawn with respect to the amendment. The 35 USC 112 second paragraph rejection of claims 1-11 have been withdrawn with respect to the amendment.

1.2 Applicant's arguments, see pages 5-9, filed on 4/23/2008, with respect to the rejection(s) of claim(s) 1-8 have been fully considered but they are not persuasive as amended. With respect to claim 1, Applicant argues that Spagna does not disclose determining whether or not program update is possible based on transmitted inherent ID of the LSI device and the application ID. Examiner respectfully disagrees as the claim does not recite the limitations as argued by applicant. Claim 1 recites two determining steps: the first one is to determine whether or not the update object program (program to be updated) may be transmitted based on device ID and application ID and another step of determining whether or not program update is possible based on the transmitted additional information. In addition, Spagna discloses identification of end user device (inherent device ID) as part of information that needs to be validated for a license in order to authorize the user to receive the content (see column 48, lines 16-18 and line 40). As interpreted by the Examiner, by verifying user identifications and providing license to users the

update object program may be transmitted (see column 26, line 66 through column 27, line 9). It is reasonable to say that the updating of the usage rights of the content described in Spagna meets the recitation of program update as Spagna discloses providing a license that specifies usage conditions that may be updated (see column 90, lines 62-67, column 95, lines 29-67), and explicitly discloses new license for modified content that also meets the claimed recitation of program update (see column 96, lines 39-48) and further discloses updating the content to be downloaded and purchased by the users (see column 77, lines 35-37 and column 21, lines 1-30). As shown above, applicant has not overcome the rejection of claim 1; therefore, claims 1-8 remain rejected in view of the prior art. Claim 1 has been amended to more particularly point out the claimed invention. Upon further consideration, a new ground of rejection is set forth below.

Claim Rejections - 35 USC § 112

2. The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

Claims 1-8 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention. Claim 1 has been amended to recite that the ID of the LSI device transmitted by the

system is an inherent ID. Examiner cannot find any section in the specification specifying the ID as an inherent ID after careful review and search.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1 and 8 are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent 7,110,984 to **Spagna et al** in view of US Patent 6,970,565 to **Rindsberg**.

As per claim 1, **Spagna et al** substantially discloses a method for updating an inherent key-encrypted program in a system including an LSI device and an external memory, the inherent key-encrypted program being generated by encryption with an inherent key unique to the LSI device and being stored in the external memory, the method comprising:

Spagna et al discloses transmitting by the system to a server (the server is not limited to any of the elements as shown in fig.1 see also column 20, line 129 through column 21, line 130) identification information that includes a content ID, application ID, user information which includes user device ID (see column 48, lines 16-40 and column 26, lines 25-35) that meets the recitation of a step of *transmitting by the system an inherent ID of the LSI device and an*

application ID which is identification information of an update object program to a server; **Spagna et al** discloses the server verifies whether or not program requested by the user should be transmitted based on the transmitted identification information as shown above and further discloses transmitted by the server additional information (such as license information) if it is determined that the update object program may be transmitted (see column 26, lines 36-55 and column 39, lines 49-67) that meets the recitation of *a step of determining by the server whether or not the update object program may be transmitted based on the transmitted inherent ID and application ID, and transmitting by the server additional information of the update object program if it is determined that the update object program may be transmitted*; **Spagna et al** discloses a step of determining by the system if program update is possible based on transmitted additional information (see column 45, lines 48-51 and column 95, lines 29-67 and column 21, lines 1-30) and further discloses requesting by the system to the server to transmit common-key encrypted content generated by encryption with a common key if it is determined that program update is possible (see column 30, lines 20-30) that meets the recitation of *a step of determining by the system whether or not program update is possible based on the transmitted additional information, and requesting by the system to the server to transmit a common key-encrypted program generated by encryption with a common key if it is determined that program update is possible;* **Spagna et al** discloses *receiving by the system a common key-encrypted program generated by encryption with a common key and transmitted from the server* (see column 30, lines 20-30); **Spagna et al** discloses *a second step of decrypting by the system the received common key- encrypted program to generate a raw program* (see column 30, lines 20-30). **Spagna et al** discloses *re-encrypting by the system the raw program with an inherent key and*

storing the re-encrypted program in the external memory as a new inherent key-encrypted program (see column 91, lines 44-61) and also discloses in column 95, lines 63-67 the option of using an external memory for storage. **Spagna et al** does not explicitly disclose the key for reencrypting is a unique key to the device. **Rindsberg** in an analogous art discloses *re-encrypting by the system the raw program with an inherent key unique to the LSI device* (see column 7, lines 33-41). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of **Spagna et al** to re-encrypt the content using unique device key as to ensure that only that device can decrypt and use the content thus providing a second level of security making the key less likely from being compromised as taught by **Rindsberg** (see column 8, lines 23-26 and column 8, line 50 through column 9, line 8).

As per claim 8, **Spagna et al** discloses receiving a hash value of the raw program transmitted from the server and the received hash value is used to perform a hash verification on the decrypted raw program (see column 41, line 49 through column 42, line 19).

4. **Claims 2, 4, 6, and 7** are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent 7,110,984 to **Spagna et al** in view of US Patent 6,970,565 to **Rindsberg** as applied to claims 1 and 8 and further in view of US Patent 6,577,734 to **Etzel et al**.

As per claim 2, both references substantially teach the claimed method of claim 1. **Spagna et al** is silent about receiving by the system common key information transmitted from

the server and generating by the system a raw common key using the received common key information. **Etzel et al** in an analogous art discloses receiving by a device shared key information transmitted from system 100 and generating a shared key using the shared key information (see column 6, lines 6-20) that meets the recitation of receiving by the system common key information transmitted from the server and generating by the system a raw common key using the received common key information and further discloses wherein at the second step, the raw common key is used to decrypt the common key-encrypted program (see column 7, lines 39-41). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method as combined above to allow each device to generate own shared key from common key information as taught by **Etzel et al** because it would avoid transmission and/or storing of the key and thereby preventing the key to be obtained by unauthorized party as suggested by **Spagna et al** (see **Spagna et al**, column 91, lines 44-53).

As per claim 4, **Spagna et al** discloses generating the key at startup and storing inherent key information in the internal memory (see column 88, lines 49-63), but does not explicitly state the system uses the inherent key information stored in the internal memory to generate a raw inherent key at boot-up of the system. **Rindsberg** discloses that each unique key (inherent key) corresponds to a unique ID and extracted upon reset (bootup) (see column 7, lines 33-41) and further discloses the raw inherent key is used for re-encrypting the raw program (see column 7, lines 36-38). **Etzel et al** in an analogous art discloses during booting generating a unique device key using device key information and stored in its secure memory to prevent tampering (see

column 3, lines 12-36). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method as combined above to allow each device to generate unique device key upon startup using inherent key information as taught by **Etzel et al** so as to securely manage the keys and prevent them from being misappropriated for fraudulent purposes (see **Etzel et al,** column 1, lines 47-50).

As per claim 6, the combination of **Spagna et al** and **Etzel et al** discloses wherein the generated raw inherent key is stored in a register of the LSI device and is used for decrypting the inherent key-encrypted program to a raw program for execution of the inherent key-encrypted program (see **Spagna**, column 39, lines 22-25 and column 30, lines 20-30).

As per claim 7, the combination of **Spagna et al** and **Etzel et al** discloses the LSI device includes a boot ROM in which a boot program is stored (see **Etzel et al**, column 9, lines 20-34); **Spagna et al** discloses external memory interface and additional interfaces or communication link and receiver for establishing data transmission with the server (see column 61, lines 24-67) that meets the recitation of external memory includes an acquisition program for establishing data transmission between the LSI device and a server; **Etzel et al** also discloses controlling update processing performed after the reception of the common key-encrypted program based on the boot program stored in the boot ROM (see **Etzel et al**, column 9, lines 20-30 and lines 50-63). Claim 7 is therefore rejected on the same rationale as the rejection of claim 2 above.

5. **Claims 3** and **5** are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent 7,110,984 to **Spagna et al** in view of US Patent 6,970,565 to **Rindsberg** in view of US Patent 6,577,734 to **Etzel et al** as applied to claims 1-2 and further in view of US Patent Publication US 2002/0116632 to **Itoh et al** *(Applicant's IDS)*.

As per claim 3, the combination of **Spagna et al, Etzel et al,** and **Rindsberg** discloses the claimed method of claim 2. Neither of the references explicitly discloses double encryption. **Itoh et al** in an analogous art discloses an encrypted common key generated by encrypting software key Ksoft with Ks2 and Ks2 generated by encrypting Ks2 with Ks1 (see page 6, paragraphs 93-95) that meets the recitation of wherein the common key information includes an encrypted common key generated by encrypting the raw common key with a raw first intermediate key, and an encrypted first intermediate key generated by encrypting the raw first intermediate key with a raw second intermediate key. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method as combined above to provide a double encrypted key as taught by allow each device to generate own shared key from common key information as taught by **Itoh et al** because having the software key dependent on two keys in a double encryption method would make the key less vulnerable against tampering.

As per claim 5, the combination of **Spagna et al** and **Etzel et al** discloses the claimed method of claim 4. Claim 5 is similar to claim 3 except for double encrypting the raw inherent key whereas claim 3 double encrypts the raw common key. **Itoh et al** discloses double

encryption as shown in claim 3 above. Therefore, claim 5 is rejected on the same rationale as the rejection of claim 3 above.

Conclusion

6. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

6.1 The prior art made of record and not relied upon is considered pertinent to applicant's disclosure as the prior art discloses many of the claimed features. (See PTO-form 892).

6.2 Any inquiry concerning this communication or earlier communications from the examiner should be directed to CARL COLIN whose telephone number is (571)272-3862. The examiner can normally be reached on Monday through Thursday, 8:00-6:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser G. Moazzami can be reached on 571-272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Carl Colin/
Primary Examiner, Art Unit 2136
July 27, 2008